Strategy Research Project

Mission Networks: An Evolution in Information Sharing

by

Lieutenant Colonel David R. Wills
United States Army

United States Army War College
Class of 2012

This manuscript is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE *(DD-MM-YYYY)* 20-03-2012	**2. REPORT TYPE** Strategy Research Project	**3. DATES COVERED** *(From - To)*

4. TITLE AND SUBTITLE

Mission Networks: An Evolution in Information Sharing

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Lieutenant Colonel David R. Wills

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Colonel Darrell Fountain
Department of Distance Education

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution A: Approved for public release distribution is unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The Department of Defense (DOD) continually seeks to produce adaptive, flexible and agile military forces responsive to the constantly changing joint, interagency, intergovernmental and multinational (JIIM) environment. Despite this effort and the operational exigencies created by U.S. involvement in multiple operations, US military forces still require operational information sharing culture capability adaptation. This paper posits that the DOD must capitalize on the recent successful adoption of the Afghanistan Mission Network (AMN) and reinforce the significant change in culture and capability represented. It will examine key strategic guidance articulating net-centric mandates, the current operating environment, and the implementation of the AMN as an example of a successful information sharing strategy based on the 'need to share'. A review of strategic guidance, policy and technology will show that they have enabled mission partner information sharing since 2005 and should be refined and strengthened based on current operational successes. The reality of declining resources and full spectrum operations in the future requires DOD to anchor the 'need to share' culture and capability to meet future operational requirements.

15. SUBJECT TERMS

Information Sharing, Mission Network, Mission Partner, Net-Centric, Organizational Behavior

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT UNCLASSIFED	**b. ABSTRACT** UNCLASSIFED	**c. THIS PAGE** UNCLASSIFED	UNLIMITED	34	**19b. TELEPHONE NUMBER** *(include area code)*

USAWC STRATEGY RESEARCH PROJECT

MISSION NETWORKS: AN EVOLUTION OF INFORMATION SHARING

by

Lieutenant Colonel David R. Wills
United States Army

Colonel Darrell Fountain
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Lieutenant Colonel David R. Wills

TITLE: Mission Networks: An Evolution in Information Sharing

FORMAT: Strategy Research Project

DATE: 22 March 2012 WORD COUNT: 6,325 PAGES: 34

KEY TERMS: Information Sharing, Mission Network, Mission Partner, Net-Centric, Organizational Behavior

CLASSIFICATION: Unclassified

The Department of Defense (DOD) continually seeks to produce adaptive, flexible and agile military forces responsive to the constantly changing joint, interagency, intergovernmental and multinational (JIIM) environment. Despite this effort and the operational exigencies created by U.S. involvement in multiple operations, US military forces still require operational information sharing culture capability adaptation. This paper posits that the DOD must capitalize on the recent successful adoption of the Afghanistan Mission Network (AMN) and reinforce the significant change in culture and capability represented. It will examine key strategic guidance articulating net-centric mandates, the current operating environment, and the implementation of the AMN as an example of a successful information sharing strategy based on the 'need to share'. A review of strategic guidance, policy and technology will show that they have enabled mission partner information sharing since 2005 and should be refined and strengthened based on current operational successes. The reality of declining resources and full spectrum operations in the future requires DOD to anchor the 'need to share' culture and capability to meet future operational requirements.

MISSION NETWORKS: AN EVOLUTION IN INFORMATION SHARING

United States (U.S.) military forces operational network, in support of Afghanistan operations, transitioned from Secret Internet Protocol Router Network (SIPRNET) to the Combined Enterprise Regional Information Exchange System (CENTRIXS)-International Security Assistance Force (ISAF) (CX-I) in 2010. The Department of Defense (DOD) implemented CX-I as the US contribution to the Afghanistan Mission Network (AMN), which constituted an unprecedented evolution of U.S. military forces culture and capability towards mission partner information sharing. This transition also marked a significant milestone in the acceptance of a culture change envisioned by former Commander, U.S. Strategic Command, General (GEN) James Cartwright in 2005. GEN Cartwright stated that multinational intelligence sharing was not technical but cultural and it represented a paradigm shift in the mindset from the 'need to know' to the 'need to share'.[1] Six years later, General Manager Georges D'hollander, the North Atlantic Treaty Organization (NATO) Consultation, Command and Control Agency (NC3A), confirmed U.S. culture in support of Afghanistan operations had changed from the traditional 'need to know' to a 'need to share': it facilitated a fundamental and "revolutionary" change in intelligence sharing.[2]

The *2001 Quadrennial Defense Review* (QDR) communicated the DOD initial information sharing requirement. Since then, strategic guidance, policy and technology have enabled the evolution of joint, interagency, intergovernmental and multinational (JIIM) mission partner information sharing. However, classic change resistance as exemplified by the firmly embedded DOD 'need to know' culture, has limited the adoption of net-centric information sharing.

In order to facilitate a ‘need to share’ culture change, the DOD must capitalize on the adoption of a mission network information sharing strategy utilized in the ISAF-Afghanistan operational network, the AMN. The successful adoption of the AMN promotes the goals of net-centric information as a viable solution for information sharing. The solution delivers efficient mission partner information sharing and establishes precedence for recapitalizing net-centric information sharing goals for a mission network information sharing strategy. How the DOD proceeds with organizational change and anchoring the ‘need to share’ information culture dictates DOD’s future ability to respond to national interests.

This paper will examine key strategic guidance articulating information sharing mandates, the evolution of net-centricity, the current operating environment, the AMN, DOD organizational change and associated risk. The AMN provides a case study for the successful implementation of the mission network strategy as an example of a successful information sharing approach based on the ‘need to share’. A review of strategic guidance, policy and technology will show that they have enabled mission partner information sharing since 2005 and should be refined and strengthened based on current operational successes. The reality of declining resources and range of military operations[3] in the future requires DOD to anchor the ‘need to share’ culture and capability to meet future operational requirements.

Strategic Guidance and the Evolution of Net-Centricity

Based upon the then recent Kosovo experience, the DOD stated in the *2001 QDR* that interoperability would enable joint and combined operations. It defined joint to include Reserve Components, civilian specialist, federal agencies, state organizations and coalition partners. It further identified a requirement for “high-capacity, interoperable communications systems that can rapidly transmit information over secure, jam-resistant data links to support joint forces."[4]

Four years into the Global War on Terrorism and Operation Enduring Freedom (OEF)–Afghanistan, the DOD revisited their interoperable, integrated and secure information sharing requirements. The DOD further highlighted information sharing requirements in the *2005 National Defense Strategy* (NDS) as a requirement for "even greater joint, interoperable command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR).[5] Interoperability and information sharing drove network-centric information sharing strategy and force transformation. The *2006 QDR* also prescribed interagency and multinational information sharing based upon net-centricity.

The President of the United States (POTUS) supported information sharing and transformation efforts by developing a sense of urgency and directing classified and unclassified information sharing with both interagency and multinational forces. In October 2005, the POTUS enacted multinational information sharing by issuing *Executive Order 13388, Further Strengthening the Sharing of Terrorism Information to Protect Americans*. It directed DOD agencies and the military Services to share classified and unclassified information with the interagency.[6] In June 2006, 4 months after the publication of the *2006 QDR*, the POTUS granted SIPRNET access to specified coalition partners emphasizing "the need for maximum sharing of classified military and intelligence information with specified coalition partners."[7]

The *2008 NDS* and *2010 National Military Strategy* (NMS) communicated requirements to integrate and improve intelligence capabilities with our allies and partners. It required the DOD to enhance its capability to integrate, synchronize actions, and communicate effectively in order to provide adaptive, flexible and speedy integration and planning to sustain global support.[8] The *2010 QDR* emphasized the requirement for better integration with civilian agencies and organizations, while working with and through allies and partners in order to prevent and deter conflict.[9]

The mature DOD concept of Net-Centricity fundamentally facilitated the successful instantiation of the AMN. The maturation of this concept over time had established essential principals and understanding throughout the communications community. The journey towards net-centricity began in earnest as basic interoperability, coupled with an emphasis on information sharing and collaboration. The more mature notion of Net-centricity was born from the recognition that mission partners had significant requirements that went beyond basic interoperability and the growing recognition that "the whole of an integrated and networked force is far more capable than the sum of its parts."[10]

Institutions in the DOD began implementing in parallel policy in support of these concepts. In May 2003, the DOD Chief Information Officer published the DOD *Net-Centric Data Strategy.*[11] In the *2005 Net-Centric Environment Joint Functional Concept 1.0*, the DoD defined the user community as mission partners to include "allies, coalition partners, international organizations, civilian government agencies, non-governmental agencies, and other non-adversaries who are involved with the activities or operations of the Joint Force."[12] Shortly thereafter, GEN Cartwright emphasized the need for greater organizational change stating that multinational intelligence sharing is "not a technical issue any more. It's really more about culture and [recognizing] the 'need to share' rather than the 'need to know.'"[13] The *2007 DOD Directive 8320.02* "*Data Sharing in a Net-Centric Department of Defense*" provided a clear definition of net-centric information sharing:

> Net-centricity is a robust, globally interconnected network environment (including infrastructure, systems, processes, and people) in which data is shared timely and seamlessly among users, applications, and platforms. Net-centricity enables substantially improved military situational awareness and significantly shortened decision making cycles.[14]

The premise for the net-centric information sharing strategy was data visibility and accessibility. This premise drove the establishment of seven goals which would facilitate net-centricity and net-centric information sharing strategy. They are

- Make data visible
- Make data accessible
- Institutionalize data management
- Enable data to be understandable
- Enable data to be trusted
- Support data interoperability
- And be responsive to user needs.

This review of strategic guidance highlights that strategic information sharing mandates have matured since the 2001 QDR while remaining consistent with initial fundamental principles. DOD has developed a strategic vision and strategy for transformation based upon leveraging technology in order to establish information superiority. Strategic guidance for the last eleven years has not altered that fundamental vision. As illustrated by DOD's information sharing evolution, supporting policy, presidential executive orders and DOD strategic guidance all supported information sharing efforts. Consistent strategic guidance provided specified and implied mandates for enhanced and expanded information sharing that created the environment for forces operating in the field to implement fundamental change. U.S. Forces deployed in support of ISAF-Afghanistan provided the operational need and visionary leadership to take advantage of that environment.

Although the drive to a Net-Centricity DOD Wanes the Conditions are Set

Empowering broad-based action entails identifying and removing the obstacles that may impede change. It requires the alignment of doctrine, policy, tactics, techniques and procedures (TTP), processes and structure with the new vision.[15] In the DOD, policy drives change; therefore, it must be aligned to the new vision first. Policy then directs the alignment of doctrine, TTP, processes and structure with the new vision.

In 2010, net-centricity references vanished from strategic guidance and some foundational policy documents did not adequately reflect net-centric ideas. A lack of detailed definitions and waning communications in strategic guidance would suggest that that despite the long communicated vision and added presidential urgency, DOD efforts never created the required momentum to generate the essential culture change and true transformation.

But sufficient changes in fundamental policy and understanding of established policy had occurred in two areas, setting the conditions for transformational success. The first area concerns the long standing *National Disclosure Policy* (NDP), governing disclosure of classified military information. It is the center of gravity for mission partner information sharing. NDP dictates what classified military information can be released and under what conditions. The second area, network and information assurance policies govern how data networks and resources facilitate information sharing and how.

NDP classified and controlled information and material not only by security classification; NDP catalogued information and material into eight categories. In light of the range of military operations and unified land operations[16], mission partner information sharing will be limited to the categories of "combined military operations, planning, and readiness" and "military intelligence, information of a military character pertaining to foreign nations."[17] In 2006, counter terrorism information sharing requirements expanded the "combined military operations, planning, and readiness" category to include combined military and counterterrorism operations.[18] Thus disclosure policy establishes the authority to disclose and share information through categorical and conditional constraints. The policy delegates the required authority to share information to the Combatant Commanders, and policy enables mission partner information sharing congruent with strategic guidance.

Network and information assurance policies govern the use of technology in the operational environment.[19] Similar to disclosure policy, network and information assurance policy has conditions, constraints and limitations regarding mission partner information sharing. Network policy identifies the roles, responsibilities and authorities for installation, operation and maintenance of technology resources. Information assurance policy establishes all aspects of protecting the confidentiality, integrity and availability of information.

The combination of *NDP* and DOD's dependence on data networks for mission command, reconnaissance and surveillance[20] and information sharing renders data networks as the primary means for information sharing. DOD's data networks facilitate two methods of mission partner information sharing in order to fulfill DOD information sharing vision. The first method simply grants mission partners' access to Defense Information Systems Network (DISN). The second method establishes network interconnections between mission partner networks and the DISN.

In the first method, when mission partners are collocated with DOD organizations, granting mission partner access is relatively straight forward. The *2002 DOD Directive 8500.1, Information Assurance (IA)*, outlines the requirements. If mission partners are not co-located with DOD organizations, DOD must first extend the DISN to the mission partner and then the DISN Designated Approving Authorities (DAAs) may grant access.

CENTRIXS is the best example of extending US resources to a mission partner and then granting them access. The Defense Information Systems Agency (DISA) Multinational Information Sharing (MNIS) extends and grants coalition or allied mission partners access to CENTRIXS networks based upon operational requirements and international agreements. DISN policy and the 2010 *CJCSI 6285.01B CH 1 Multinational Information Sharing (MNIS) Operational Systems Requirements Management Process* establish the policy to extend DISN and CENTRIXS resources. Both policy and regulatory guidance enable mission partner information sharing.

The second method, method establishes network interconnections between mission partner networks and the DISN, is subject to the policy that authorizes the access and extension of DISN networks. Justifications must be operationally compelling, and not one of convenience. It consists of the interconnection of "DoD information systems of different security domains or with other U.S. Government systems of different security domains,"[21] and must comply with all policies to include information insurance (IA) policy.

IA policy includes approved hardware and software, configuration, training, configuration control and access control. *DoD 8500.1* additionally authorizes the "interconnection of DoD information systems with those of U.S. allies, foreign nations, coalition partners, or international organizations."[22] All interconnections must support operational information exchange requirements (IER) and comply with all policies and international agreements.[23] A critical component to the interconnection of systems or networks consisting of different security domains is for the DISN DAAs to ensure the implementation of mitigation measures for risks identified with the connection;[24] they must also comply with *DoD Directive O-8530.1 Computer Network Defense (CND).* Interconnections to sensitive compartmented information (SCI) systems or networks must comply with *Director of Central Intelligence Directive (DCID) 6/3*.[25] All DOD information systems must comply with established policies to include *DoD Instruction 8510.01DoD Information Assurance Certification and Accreditation Process (DIACAP*) and *DoD Instruction 8100.3 Department of Defense (DOD) Voice Networks*.[26]

Leadership Recognizes the Need for a New 'Mission Network'

In 2008, 44 troop contributing nations (TCNs) contributed to ISAF-Afghanistan's increasing complex JIIM operations. This drove US military forces to seek a true change in the operational environment's culture from that of 'need to know' to 'need to share.' Regional Command (RC)-East Headquarters identified18 information exchange requirements in order to share information as well as mission command among ISAF and U.S. Forces in RC-East. In January 2009, US Forces Afghanistan (USFOR-A)

Commander, GEN David D. McKiernan, formally identified the requirement for an operational network that was fully integrated and enabled robust information exchange among all ISAF and US Forces. He requested approval to interconnect US CENTRIXS-GCTF and NATO ISAF SECRET networks. By that time, he had identified cross-domain solutions between networks as restrictive, and unreliable, thus contributing to poor information flow and impeding ISAF's ability to perform mission command of forces. He also recognized that the FY 2009 Troop Surge and expansion of US Forces in RC-South would only exacerbate the problem.[27] In August 2010, U.S. Central Command (USCENTCOM) and NATO interconnected CENTRIXS-ISAF to NATO ISAF SECRET, creating the AMN - the operational network for ISAF. The AMN is a plug-and-play network modeled after the internet that facilitates rotational ISAF troop contributing nations' ability to connect their national secret REL ISAF networks, which, in turn, allows commanders and their staffs to execute mission command of ISAF over the AMN. Troop contributing nations' national secret networks would become secondary and facilitate communications between troop-contributing nation's military leadership and their own operational or strategic leadership. To date, ten troop-contributing nations have contributed to and connected to the AMN.

Currently the AMN hosts 87000 users that represent 49 nations. The Afghanistan Mission Network Operation Center (AMNOC) and five regional command network operation centers along with 13 service desks together provide user, network and systems support, operation and maintenance. The AMN provides more than 75 services that consist of watch lists, applications or functional area systems with 529 computer information systems points of contacts are responsible for these services.[28]

During the 2011 Technology Symposium, Mr. Georges D'hollander, General Manager, the NATO Consultation, Command and Control Agency (NC3A), addressed the conference with a speech entitled *the Afghanistan Mission Network (AMN) Reaping the Rewards of Network-Enabled Operations.* During the presentation, Mr. D'hollander proclaimed the standup of the AMN as truly revolutionary. The AMN influenced a culture change from the traditional ‘need to know’ to a ‘need to share’ facilitating a fundamental change in intelligence sharing.[29]

Current Operating Environment

Joint Publication 6-0 Joint Communications System states that the Global Information Grid (GIG) composed of the Defense Information Systems Network (DISN) and other networks tunneled over the DISN “supports effective coordination and liaison with those activities of the U.S. Government outside the DOD that have functions associated with the”[30] National Military Command System (NMCS). Effective coordination translates into business collaboration services of chat, email, web and Voice over Internet Protocol (VoIP). The DoD branch of the United States government utilizes the ’.mil’ sub-network of the GIG while the other branches of the United States Government (USG) such as the Department of State (DoS) utilize the ’.gov’ sub-network of the GIG. The result is that unless the DOD has a ’need to know’ it will never have access to the DOS information that resides on the ’.gov’ sub-network of the GIG or vice versa.

Given the ‘need to know’ culture designed into the GIG and ingrained in the U.S. Military Services, Combatant Commands and subordinate units, intergovernmental sharing is technologically and organizationally formidable. The information assurance goals set in place to ensure information confidentiality, integrity and availability reinforce the ‘need to know’ mindset from the senior leadership to the smallest organizations in U.S. military forces. As a result, individuals and organizations are inherently compelled not to employ net-centric principals that make data visible, accessible, understandable, trusted and interoperable. Ironically, the impacts of ‘need to know’ culture and information assurance are fundamentally counterintuitive to reasons for the construction and expansion of the modern information networks: information highways emerged in order to interchange information.[31]

The result has been limited mission partner information sharing during Military Operations Other Than War (MOOTW), Full Spectrum Operations and now Unified Land Operations over the last 21 years (1991 – 2012). These operations include JIIM operations such as humanitarian assistance (HA), disaster relief, nation assistance, foreign internal defense (FID), counterdrug operations, arms control, defense support to civil authorities (DSCA)[32], noncombatant evacuation and repatriation operations (NEO) and peacekeeping operations. After Action Reports, (AARs) collected after these various types of operations, stated the requirement for improved mission partner information sharing.

Operational necessity has increasingly demanded mission partner information sharing over the past 21 years, and as a result the DOD attempted two solutions for sharing information and providing near-real time services, mission command, reconnaissance and surveillance to mission partners. The DOD developed cross-domain solutions and U.S. Title X multilateral and bilateral networks. The first option, cross-domain solutions exchange information between networks of different security domains; however, the use of cross-domain solutions requires testing, accreditation, installation, certification, operation and maintenance. The skills required to operate and maintain cross-domain solutions are highly specialized and expensive. Depending on the location of the cross-domain solution, the type and amount of data migrated introduces unacceptable delays that impede mission partner use of data. While cross-domain solutions work well for email and other non-real-time applications, applications such as Blue Force Tracking (BFT) that is dependent upon near-real time data suffer from problematic time delays. Business collaboration applications are also challenged by the implementation of cross-domain solutions. The maintenance of appropriate security markings during the information exchanges between security domains can be exceptionally problematic.

Recognizing the information sharing limitations of cross domain solutions, the DOD offers CENTRIXS multinational information sharing networks as its second solution. CENTRIXS is the primary means to share information rapidly with coalition partners worldwide across combined forces and unified commands for planning, unity of effort, decision superiority and decisive global operations.[33] Although CENTRIXS networks share information with intergovernmental and multinational mission partners, information producers share information based fundamentally on a ‘need to know’ culture. The DoD provides ‘need to know’ information through collaboration services of Electronic mail (Email) with attachments, Web-enabled services, office automation, bulletin boards, chat service (collaboration services) and Voice over Internet Protocol (VoSIP), near-real-time data access, Common Operational Picture (COP) and Common Intelligence Picture (CIP).[34] Multinational and bilateral partners consume CENTRIXS provided information in DOD formats through DOD systems. The result is that data is not produced with the goals of net-centricity embedded. Data produced on CENTRIXS networks is not readily visible, accessible, understandable or trustable to a mission partner's network, nor does it support data interoperability.

North Atlantic Treaty Organization (NATO) International Security Assistance Force (ISAF) – Afghanistan Case Study

DoD SIPRNET, CENTRIXS-GCTF or cross-domain solutions did not conform to net-centric information sharing goals and therefore did not facilitate mission partner information sharing in Afghanistan. USCENTCOM and NATO, as members of the AMN COI, focused on enabling 'need to share' capability through net-centric information sharing goals. The AMN architecture began with the ISAF Commander's operational requirements identified by battle tasks or mission essential task lists (METL). The U.S. Joint Forces Command (JFCOM) Universal Joint Task List (UJTL) provides a menu of tactical, operational and strategic mission threads from which Commanders derive battle or METL tasks. Analysis of identified mission threads produced information exchange requirements associated to tasks, a list of applications and systems that would facilitate each required exchange. The resultant product was a service catalogue supporting mission partner mission threads. A complete analysis of the Universal Joint Task List produced a menu of services that identifies applications and systems required for IER and task accomplishment by mission thread. The service menu concept facilitates mission network applications and systems selection that are specific to individual JIIM operations responsive to the user requirements.

A systems architecture designed in this fashion that identifies IER, tasks, mission threads, applications and systems inherently facilitates data management. Analysis of the systems architecture identifies producers and consumers of information. The distinction enables the identification of trusted producers and the production of authoritative data sources. Goals to make data visible, accessible, understandable, and interoperable enable authoritative data sources to produce data which can be stored once and utilized repeatedly. Data management facilitates the most efficient use of data and its resources.

The AMN COI utilized a combination of meta-data tagging and federated data bases to make data visible. In order to make data accessible, the AMN COI implemented security measures that facilitated the data exchange among the applications, systems and networks identified in the AMN architecture. Additionally, the AMN COI ensured that the data was understandable and interoperable based upon data standards. As a result, the AMN COI agreed upon the following data standards: Multilateral Interoperability Program (MIP)/Joint Consultation, Command and Control Information Exchange Data Model (JC3IEDM), Extensible Messaging and Presence Protocol (XMPP), web GIS, Data Dissemination Service (DDS)/Publish and Subscribe Services (PASS) schemas and web services.

By recognizing and utilizing net-centric information sharing goals, the AMN COI developed an ISAF SECRET World Wide Web capability that is based fundamentally on a ‘need to share’. The AMN facilitated the development by each ISAF troop contributing nation of its own national ISAF SECRET contribution to the AMN. It allowed each nation to utilize its own applications and systems that would meet the AMN data standards, reducing training and maximizing potential expertise and proficiency. The AMN enabled strategic flexibility for partner nations to start as the strategic, operational or tactical lead and transition to other roles during ongoing operations. It further established integrated control that would enable unity of effort, purpose and action among diverse organizations and agencies. This unity of effort facilitated significant operational efficiencies and allowed all mission partners to realize the true value of effective JIIM operations. The AMN clearly enabled mission partner information sharing specific to ISAF-Afghanistan.

Organizational Change

It has taken 11 years to develop an information sharing strategy that facilitated organizational change from ‘need to know’ to ‘need to share’ in U.S. military forces in Afghanistan, accounting for only a fraction of the DoD enterprise. DOD issued its first ‘need to share’ guidance in the *2001 QDR*;

> The effectiveness of these operations will depend upon the ability of DOD to share information and collaborate externally as well as internally. Interoperability, which enables joint and combined operations, is a key element in all DOD operational and systems architectures.[35]

The DOD has maintained and reinforced this position in subsequent strategic messages to include the *2012 Defense Strategic Guidance*. It states that U.S. Joint Force “will be agile, flexible, ready and technologically advanced. It will have cutting edge capabilities, exploiting our technological, joint and networked advantage.”[36] The DOD has made progress in providing data to mission partners through cross-domain solutions (CDS) and CENTRIXS networks,; however, these solutions were designed primarily to provide mission partners with information based on a ‘need to know’. Little has changed since the *2001 QDR*.

Resistance to change is a common phenomenon observed in any organization. However, the DOD must change its organizational culture to ‘need to share’ in order to achieve the joint and networked advantage. The operational use of SIPRNET has firmly entrenched a ‘need to know’ culture in the DOD over the last 21 years, which is not conducive to ‘need to share’ culture change. John P. Kotter’s eight step process for creating major change provides a detailed framework. Kotter’s change process consists of:

- Establishing a sense of urgency
- Creating the guiding coalition.
- Developing a vision and strategy
- Communicating the change vision
- Empowering broad-based action
- Generating short-term wins
- Consolidating gains and producing more change
- Anchoring new approaches in the culture[37]

Kotter’s framework facilitates the following analysis of DOD’s initiative to change its information sharing paradigm from ‘need to know’ to a more expansive concept. A cursory review of relevant DOD strategic documents and initiatives reveals that the initial steps toward change were taken. The net-centric strategy, published by the DoD CIO, was developed in 2003 and evolved through the years until 2010. Subsequent policy followed that empowered broad-based action to support joint, interagency, intergovernmental and multinational (JIIM) information sharing. The POTUS established a sense of urgency through executive orders which directed classified and unclassified information sharing with both interagency and multinational forces.

Unfortunately, initial incremental efforts to expand information sharing focused on cross-domain solutions and the deployment of CENTRIXS; fundamentally designed with the classic ‘need to know’ mindset. These efforts while mildly successful at expanding the ability to share key elements of organizational information, did not generate the level of integrated information sharing envisioned or required to move DOD to truly more effective JIIM operations. Often the operational community accepted these incremental information-sharing improvements as good enough. Thus, these perceived short-term ‘wins’ were consolidated and began to be institutionalized stymieing real change to a more effective model.

DOD efforts never generated compelling results to produce an effective information sharing model; the DOD lost its sense of urgency. It subsequently abandoned its net-centric information sharing strategy; it neglected to identify a new information sharing strategy; and it failed to establish a JIIM information sharing environment. Additionally, no evidence exists to support that the DOD established a guiding coalition that would encourage JIIM information sharing. Until recent operations in Afghanistan, SIPRNET remained the DOD operational network and subordinate services had not moved to a set of new information sharing approaches. The preliminary analysis indicates that organization behavior did not change from ‘need to know’ to ‘need to share’ culture within the DOD enterprise.

ISAF’s implementation of the AMN, however, offers an example of successful organizational information sharing change. ISAF leadership seeing the need for a more expansive information sharing model established a true sense of urgency for the command with concrete objectives; the AMN’s initial operational capability (IOC) had to be available for the Fiscal Year (FY) 2010 troop increase. These objectives were further reinforced with the establishment of a formal a guiding coalition, the AMN community of interest (COI), which consisted of the empowered representatives of DOD, USCENTCOM, NATO, NC3A and the United Kingdom's (UK) Permanent Joint Headquarters (PJHQ). The COI developed a vision and strategy and communicated the change through a detailed plan of action and with milestones (POA&M), briefings, conferences, white papers, warning orders and operation orders. The DOD, USCENTCOM, NATO, NC3A and PJHQ further empowered and resourced their national representatives for broad-based action as their representatives to the AMN COI and the ISAF Accreditation and Security Board (ISAB). The empowered COI was thus able to generate tangible forward progress through the development of an architecture, service catalogue, service migration prioritization, initial operating capability objectives and clearly articulated full operational capability (FOC) end state. The sense of urgency and empowerment allowed the resourced COI to consolidate early gains and generate additional forward progress. The AMN represents the tangible instantiation of the US military forces, in Afghanistan, transition to a fully facilitated, resourced 'need to share' environment, and established a new operational precedent for fully supported information sharing in a JIIM environment.

Necessity in the operational environment, vision, strategy and most importantly leadership established the conditions for success that allowed ISAF to implement the AMN and change culture in Afghanistan. Observations of the differences between the ISAF and the DOD information sharing environments indicate that DOD senior leadership did not stay involved to sponsor the change effort throughout each step. Senior leadership did not maintain a sense of urgency towards JIIM information sharing; they allowed cross-domain solutions and CENTRIXS networks to preserve the status quo - ‘need to know’ culture. They did not select a guiding coalition whose members came from different levels within the DOD with authority, credibility, expertise, and leadership responsibilities and understood the change vision and the operational requirement for change. Senior leadership as well as the guiding coalition did not appropriately identify the new behavior, attitudes and skills that operational and tactical leaders and users required in a JIIM environment; “align with the behavior, attitudes, and skills that are needed for the change effort.”[38] Although, policy empowered broad based action, it was not enough. Senior leadership must act on that policy to change doctrine, TTP, processes or structure to support JIIM information sharing operations. Too many change efforts suffer due to the lack of detailed analysis and planning, and most importantly senior leadership involvement.

Risk

The current more widely sanctioned information-sharing methods of cross-domain solutions and CENTRIXS networks expand but still limit truly effective information sharing. Furthermore, the cost to the US to lead full spectrum operations around the world in this manner, consistently being the largest contributor of enabling resources during operations is increasingly prohibitive. Review of mission networks strategy for adequacy, feasibility acceptability, and compliance with joint doctrine[39] would indicate that it is an executable mission partner information sharing strategy. Information sharing strategic guidance and policy review, in this document, indicates that a mission network strategy complies with joint doctrine. Only a future analysis of a mission network strategy that utilizes the joint capabilities integration and development system (JCIDS) doctrine, organization, training, materiel, leadership and education, personnel and facilities (DOTMLPF) framework will provide a completeness review.

Feasibility[40] analysis addresses the availability of resources. Initially, each mission network will require its own physical infrastructure. One method is to recapitalize tactical SIPRNET capabilities in order to provide a generic secret network capability. The CJTF commander can classify the network upon notification of deployment for an operation. If SIPRNET is required, the unit can tunnel the few instantiations of SIPRNET through the mission network.

Adequacy[41] analysis addresses whether or not mission networks supports key strategic guidance to improve economies of scale, build coalition partnerships and build adaptable organizations. The AMN demonstrates that mission networks establish integrated control enabling unity of action, effort, and purpose among rotational JIIM mission partners. Real improvements in operational efficiencies, force productivity and the inherent value of true JIIM operations readily demonstrate meeting stated strategic partnership goals. A particularly poignant example is plug-and-play mission command, provisioning flexible mission command transition among multinational forces.

Acceptability[42] analysis addresses the cost and benefits of the mission network concept. The increasingly constrained fiscal environment and recent operational successes clearly support the continued evolution and acceptance of the ‘need to share’ information sharing culture. DOD stakeholders required to use and defend information will resist; but tangible successes and the ability to readily refocus efforts from protecting the exclusive ‘need to know’ and transitioning to a successful governance and accountability paradigm of ‘need to share’ offer a viable way ahead.

Today in Afghanistan, ISAF has realized the benefits of organizational change with respect to information sharing by implementing mission networks. In this case the benefits of sharing with JIIM partners are readily demonstrating that they outweigh the risks associated with sharing military classified information for the purposes of "Combined Military Operations, Planning, and Readiness" and "Military Intelligence, information of a military character pertaining to foreign nations." The United States needs the ability to respond effectively in support of national interests in a collaborative environment with coalition mission partners. The true risk that the DOD accepts by not institutionalizing mission networks lies in the increasing probability of coalition operations in an ever more resource constrained environment. The DOD needs to consider risks from a larger perspective as outlined by the range of military operations. Failure to change organizational culture and implement mission networks will negatively impact future operational capabilities supporting force management, institutional, future challenges, strategic and political risks.[43]

Key operational risks include providing the capability to fully leverage the JIIM operational environment, maximizing JIIM partnership capacity, trust, unity of action, control and effort. Operational Forces continued reliance on SIPRNET will limit JIIM partner's ability to properly understand the operational environment and serve to unnecessarily isolate mission partners during JIIM operations. This isolation of US leaders, soldiers and mission partners clearly violates the Army's fundamental training principles of train as you fight and train to develop agile leaders and organizations. Leaders and Soldiers cannot fully and most effectively assess the operational environment without the collective inputs and perspectives of all participating mission partners. Limiting our leader's and Soldiers ability to properly assess and understand the operational environment when more effective alternatives are available is simply unacceptable. Failure to assess and understand the operational environment results in poor adaptation and violates the Army's Unified Land Operations founding principles of flexibility, integration, lethality, adaptability, depth, and synchronization.

Strategic risk is dependent upon military risks; it is the DOD's ability to execute military and defense strategies in support of national security interests. Without the capability to fully build the most effective JIIM partnership capacity, the DOD's capability to protect our national interest is unnecessarily compromised. As the DOD reduces the size of its forces, the US must build partnerships with other nations in order to economically meet its worldwide responsibilities and maintain its ability to export democracy. The inability to partner to the fullest and most effective extent possible represents risk to the US ability to resource, execute and sustain military operations around the world.

The DOD can mitigate the above risk through real change to its organizational information culture. The adoption of the 'need to share' concept and the implementation of a network methodology that facilitates mission partner information sharing have the potential to reduce multiple risks. Political risks are reduced by improving international and domestic perspectives of our nation's ability and determination to meet future challenges collaboratively. Repeated successful coalition operations will significantly enhance the perceived legitimacy of US actions through fully developing allies and coalition partners' capabilities and fostering trust among them. The DoD can reduce domestic risk by building public support for exercising worldwide responsibilities through increasing multinational participation and reduced US resource consumption.

Conclusion

Since, 2001 the DOD has attempted to improve its information sharing capabilities. In 2005, GEN Cartwright assessed the challenge as an organizational requirement to change DOD information sharing culture from the 'need to share' to the 'need to know.'[44] Repetitive strategic guidance implies that the DOD has remained consistent but not successfully accomplished the goals of mission partner information sharing in JIIM operations. Kotter's eight step process for creating organizational change highlights areas where the DOD can focus in order to anchor recent successful instantiations of the 'need to share' information culture within its enterprise.

The DOD has clearly established vision and has communicated that vision for the last eleven years culminating in a set of principles called net-centricity. Concurrently, mission partner information sharing has been authorized and supported by policy that empowers broad based action. Unfortunately, the lack of clearly successful net centric operations created the perception that net centricity was not an effective concept. DOD appeared to have failed to establish and maintain the sense of urgency required to move towards fully successful mission partner information sharing. The DOD did not obtain sufficient short-term wins and consolidate those wins in order to maintain forward progress.

How the DOD proceeds with completing the ongoing organizational change in information sharing culture and anchoring 'need to share' will dictate its future. The DOD realizes that it wants the strategic flexibility to start as the strategic, operational or tactical lead and transition lead during ongoing operations. Fiscal constraints and worldwide political realities dictate that DOD moves beyond the mere espousal of operating as a true coalition partner to enacting and executing the mission partner information sharing. The U.S. must realize the operational efficiencies, gains and value of true JIIM operations in an information environment that provisions near-real time coordination, integration and synchronization, which in turn establishes unity of purpose, effort and action.

The use of SIPRNET has entrenched the ‘need to know’ culture in the DOD over the last 21 years. There are many examples where the U.S. norm of fighting on SIPRNET creates strategic, operational and tactical constraints or limitations. DOD needs to review its use of SIPRNET now within the enterprise and should consider reviewing its net-centric strategy and goals as well. If the growing number of users and contributing nations to the AMN are measures of success, then the DOD should carefully review and reinvigorate the goals of net-centric information sharing.

USCENTCOM and NATO developed the AMN, utilizing the goals of net-centric information sharing as guiding principles in order to avoid installing cross-domain solutions known to be of limited effectiveness. It is the product of a network design methodology based on full mission partner information sharing that facilitates ‘need to share’ behavior. The ‘need to share’ mindset facilitates the concept of plug-and-play mission command, provisioning flexible mission command transition among multinational forces. It enables supporting nations to assume or transfer mission command of an operation without the constraints of technology implemented by a particular coalition or ally nation.

Future mission networks should continue to leverage sound net-centric information sharing goals. Communicators supported by visionary leadership must build networks that reflect CJTF user requirements and battle tasks and promote the capability to build a mission network comprised of applications and systems tailored to the operation. And most of all, mission networks must reflect ‘need to share’ while maintaining appropriate information assurance. Through the consolidation of gains in efficiency and more importantly effectiveness, ultimately “joint multinational coalition information sharing, mission command and C4ISR” based on a ‘need to share’ will be embedded in U.S. military operations culture.[45]

Endnotes

[1] U.S. Joint Chiefs of Staff, *Joint Intelligence,* Joint Publication 2-0 (Washington, DC: U.S. Joint Chiefs of Staff, June 22, 2007), V-2.

[2] NATO Consultation, Command and Control Agency (NC3A) General Manager Georges D’hollander, “The Afghanistan Mission Network (AMN) Reaping the Rewards of Network-Enabled Operations,” September 1, 2011, http://www.nc3a.nato.int/SiteCollectionDocuments /GM's%20Koblenz%20IT%20Speech%202011%20reviewed%20GM.pdfnDocuments/GM's%20 Koblenz%20IT%20Speech%202011%20reviewed%20GM.pdf (accessed November 6, 2011).

[3] The ―range of military operations‖ replaces both ―spectrum of conflict‖ and ―operational themes‖ used in the superseded FM 3-0 and FM 3-0, Change 1. ―Range of military operations‖ is the joint way of portraying the operational environment and a conflict continuum. ―Spectrum of conflict‖ and ―operational themes‖ should no longer be used. (These constructs are not formally defined terms.) U.S. Army Combined Arms Center, *Doctrine Update, 1–12* (Fort Leavenworth, Kansas: Mission Command Center of Excellence, December 16, 2011), 8.

[4] Donald H. Rumsfeld, *Quadrennial Defense Review* (Washington, DC: U.S. Department of Defense, February 2001), 45.

[5] Donald H. Rumsfeld, *the National Defense Strategy of the United States of America* (Washington, DC: Office of the Secretary of Defense, Mar 2005) 18.

[6] U.S. Joint Chiefs of Staff, *Joint Communications System,* Joint Publication 6-0 (Washington, DC: U.S. Joint Chiefs of Staff, June 10, 2010), III-10.

[7] U.S. Joint Chiefs of Staff, *Policy for the Release of Joint Information*, Chairman of the Joint Chiefs of Staff Instruction 5714.01C (Washington, DC: Washington, DC: U.S. Joint Chiefs of Staff, August 28, 2006), 2.

[8] Barack Hussein Obama, *National Security Strategy* (Washington, DC: The White House, May 2010), 5.

[9] Robert M. Gates, *Quadrennial Defense Review* (Washington, DC: U.S. Department of Defense, February 2010), i.

[10] Donald H. Rumsfeld, *the National Defense Strategy of the United States of America* (Washington, DC: Office of the Secretary of Defense, Mar 2005) 17.

[11] A. K. Cebrowski, *The Implementation of Network-Centric Warfare* (Washington, DC: Director, Office of Force Transformation, Office of the Secretary of Defense, January 5, 2005), http://www.carlisle.army.mil/DIME/documents/oft_implementation_ncw[1].pdf, (accessed September 14, 2011), 23.

[12] U.S. Department of Defense, *Net-Centric Environment Joint Functional Concept 1.0*, Department of Defense Directive 5230.11 (Washington, DC: U.S. Department of Defense, April 7, 2005), 2.

[13] U.S. Joint Chiefs of Staff, *Joint Intelligence,* Joint Publication 2-0 (Washington, DC: U.S. Joint Chiefs of Staff, June 22, 2007), V-2.

[14] Directive 8320.02, *Data Sharing in a Net-Centric Department of Defense*, 2004 (Certified Current as of April 23, 2007), 8.

[15] Robert Tanner, *Leading Change (Step 5): Empower Broad Based Action*, April 20, 2011, http://managementisajourney.com/2011/04/leading-change-step-5-empower-broad-based-action/, accessed 19 March 2012.

[16] Unified land operations replaces full spectrum operations as the Army's operating concept. Decisive action replaces full spectrum operations as the collective term for simultaneous offense, defense, stability and defense support of civil authorities. Full spectrum operations is obsolete and should be stricken from use. Whether authors use unified land operations or decisive action will depend on context and meaning. U.S. Army Combined Arms Center, *Doctrine Update, 1–12* (Fort Leavenworth, Kansas: Mission Command Center of Excellence, December 16, 2011), 8.

[17] U.S. Department of Defense, *Disclosure of Classified Military Information to Foreign Governments and International Organizations ENCLOSURE 2*, Department of Defense Directive 5230.11 (Washington, DC: U.S. Department of Defense, June 16, 1992), 15-16.

[18] U.S. Joint Chiefs of Staff, *Policy for the Release of Joint Information Enclosure A*, Chairman of the Joint Chiefs of Staff Instruction 5714.01C (Washington, DC: Washington, DC: U.S. Joint Chiefs of Staff, August 28, 2006), A-2.

[19] *Operational environment* replaces the term *battlespace,* which was frequently misused as a synonym for *area of operations*. *Battlespace* is obsolete and should not be used at all. Further, *operational environment* is not synonymous with *area of operations*. *Operational environment* does not refer to a piece of ground denoted by boundaries and assigned to a unit, nor does it refer to the security environment at large. U.S. Army Combined Arms Center, *Doctrine Update, 1–12* (Fort Leavenworth, Kansas: Mission Command Center of Excellence, December 16, 2011), 8.

[20] Mission command replaces the Army doctrinal term command and control. The former command and control warfighting function is now called the mission command warfighting function—not command and control or C2. The function of command and the function of control are still valid, but not when combined into a single phrase or function. When discussing Army operations, command and control (including the shortened form C2) is an obsolete term.
In Army doctrine, the term intelligence, surveillance, and reconnaissance (ISR) is obsolete. Army doctrine will not use this term or acronym to describe Army operations. The individual components will be spelled out. Specifically, Army doctrine will use reconnaissance and surveillance to refer to the collection of information. U.S. Army Combined Arms Center, *Doctrine Update, 1–12* (Fort Leavenworth, Kansas: Mission Command Center of Excellence, December 16, 2011), 8-9.

[21] U.S. Department of Defense, *Information Assurance (IA)*, Department of Defense Directive 8500.1 (Washington, DC: U.S. Department of Defense, October 24, 2002), 6.

[22] U.S. Department of Defense, *Information Assurance (IA)*, Department of Defense Directive 8500.1 (Washington, DC: U.S. Department of Defense, October 24, 2002), 7.

[23] U.S. Department of Defense, *Information Assurance (IA)*, Department of Defense Directive 8500.1 (Washington, DC: U.S. Department of Defense, October 24, 2002), 7.

[24] U.S. Department of Defense, *Information Assurance (IA)*, Department of Defense Directive 8500.1 (Washington, DC: U.S. Department of Defense, October 24, 2002), 6.

[25] U.S. Joint Chiefs of Staff, *Defense Information System Network (DISN): Policy and Responsibilities*, Chairman of the Joint Chiefs of Staff Instruction 6211.02C (Washington, DC: Washington, DC: U.S. Joint Chiefs of Staff, July 9, 2008, 1988), 16 (A-4).

[26] U.S. Joint Chiefs of Staff, *Defense Information System Network (DISN): Policy and Responsibilities*, Chairman of the Joint Chiefs of Staff Instruction 6211.02C (Washington, DC: Washington, DC: U.S. Joint Chiefs of Staff, July 9, 2008, 1988), 14 (A-2).

[27] USFOR-A Memorandum for Commander United States Central Command, Subject: Afghanistan Mission Network Statement of Requirements, 28 January 2009.

[28] Commander Howard Tweedie, UK Royal Marines, *Afghanistan Mission Network*, *AMN Secretariat Brief for the NATO Consultation, Command and Control Board (NC3B)*, briefing slides, March 5, 2012.

[29] NATO Consultation, Command and Control Agency (NC3A) General Manager, speech entitled “The Afghanistan Mission Network (AMN) Reaping the Rewards of Network-Enabled Operations,”2011 Technology Symposium.

[30] U.S. Joint Chiefs of Staff, *Joint Communications System*, Joint Publication 6-0 (Washington, DC: U.S. Joint Chiefs of Staff, June 10, 2010), V-2.

[31] Mitch Waldrop, “DARPA and the Internet Revolution,” in *DARPA (Defense Advanced Research Project Agency) - 50 Years of Bridging the Gap*, (Washington, DC: Defense Advanced Research Projects Agency, 2009) http://www.darpa.mil/WorkArea/DownloadAsset.

aspx?id=2554 (accessed March 5, 2012), 4.

[32] Defense support of civil authorities (DSCA) replaces civil support, consistent with joint doctrine. This is a one-for-one replacement. U.S. Army Combined Arms Center, *Doctrine Update, 1–12* (Fort Leavenworth, Kansas: Mission Command Center of Excellence, December 16, 2011), 8.

[33] JTIC Home Page, "*JITC Multinational Information Sharing (MNIS),"* http://jitc.fhu.disa.mil/dcr/mnis.html (accessed January 16, 2012).

[34] JTIC Home Page, "*JITC Multinational Information Sharing (MNIS),"* http://jitc.fhu.disa.mil/dcr/mnis.html (accessed January 16, 2012).

[35] Donald H. Rumsfeld, *Quadrennial Defense Review* (Washington, DC: U.S. Department of Defense, February 2001), 46.

[36] Leon E. Panetta, *Sustaining U.S. Global Leadership: Priorities for 21st Century* Defense (Washington, DC: U.S. Department of Defense, January 5, 2012), 5.

[37] John P. Kotter, *Leading Change* (Boston, Massachusetts: Harvard Business School Press, 1996), 21.

[38] Robert Tanner, *Leading Change (Step 5): Empower Broad Based Action*, April 20, 2011, http://managementisajourney.com/2011/04/leading-change-step-5-empower-broad-based-action/, accessed 19 March 2012.

[39] U.S. Joint Chiefs of Staff, *Joint Operation Planning*, Joint Publication 5-0 (Washington, DC: U.S. Joint Chiefs of Staff, August 11, 2011), IV-46.

[40] U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Terms*, Joint Publication 1-02 (Washington, DC: U.S. Joint Chiefs of Staff, November 8, 2010), 127.

[41] U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Terms*, Joint Publication 1-02 (Washington, DC: U.S. Joint Chiefs of Staff, November 8, 2010), 4.

[42] U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Terms*, Joint Publication 1-02 (Washington, DC: U.S. Joint Chiefs of Staff, November 8, 2010), 1.

[43] Robert M. Gates, *Quadrennial Defense Review* (Washington, DC: U.S. Department of Defense, February 2010), 89 (112).

[44] U.S. Joint Chiefs of Staff, *Joint Intelligence,* Joint Publication 2-0 (Washington, DC: U.S. Joint Chiefs of Staff, June 22, 2007), V-2.

[45] John P. Kotter, *Leading Change* (Boston, Massachusetts: Harvard Business School Press, 1996), 21.